IN THE CLAIMS

Please amend the claims as follows:

1-28. (Cancelled)

29. (Previously Presented) A method for verifying a user and a user computer comprising:

receiving at a first server at least one first message from the user computer, the at least one first message including a first fingerprint file;

comparing the first fingerprint file against a second fingerprint file to verify the user computer, the second fingerprint file accessible by the first server;

receiving at a second server at least one second message from the user computer, the at least one second message including a first identification for the user; and

comparing the first identification for the user against a second identification for the user to verify the user, the second identification for the user accessible by the second server.

30. (Currently Amended) A method according to claim 29, wherein ~~where~~ at least one of the first server and the second server is a mini-server.

31. (Currently Amended) The method according to claim 30 ~~where~~, wherein the first and second servers are mini-servers.

32. (Previously Presented) A method according to claim 31, wherein the first mini-server is associated with a first clearinghouse computer and the second mini-server is associated with a second clearinghouse computer.

33. (Previously Presented) A method according to claim 31, wherein the first mini-server is associated with a first clearinghouse computer and the second mini-server is associated also with the clearinghouse computer.

34. (Currently Amended) A method according to claim 29 further comprising: ~~, wherein:~~

after the ~~step of~~ comparing of the first fingerprint file against the second fingerprint file to verify the user computer, generating a first-mini-server message at the first mini-server based upon the results of said comparison; and

after the ~~step of~~ comparing of the first identification for the user against the second identification for the user to verify the user, generating a second-mini-server message at the second mini-server based upon the results of said comparison.

35. (Currently Amended) A method according to claim 34, further comprising ~~including~~:

sending the first-mini-server message to a vendor computer; and

sending the second-mini-server message to the vendor computer.

36. (Currently Amended) A method according to claim 35, further comprising ~~including~~:

authorizing an action by the vendor computer only if both the first-mini-server message contains information indicating the user computer was verified and the second-mini-server message contains information indicating the user was verified.

37. (Currently Amended) A vendor computer comprising:

a first input unit ~~for communicating~~ to communicate with a first ~~mini-~~server ~~for receiving~~ and to receive a first ~~-mini-~~server message containing information indicating if a user computer was verified;

a second input unit ~~for communicating~~ to communicate with a second ~~mini-~~server ~~for receiving~~to receive a second ~~-mini-~~server message containing information indicating if a user was verified;

a processor ~~for receiving~~ to receive the first ~~-mini-~~server message from the first output and the second ~~mini-~~server message from the second output and ~~authorizing~~ to authorize an action only if both the first ~~-mini-~~server message contains information indicating the user computer was verified and the second ~~-mini-~~server message contains information indicating the user was verified.

38. (Currently Amended) A vendor computer according to claim 37, wherein the first input unit and the second input unit are the same.

39. (New) The vendor computer according to claim 37, wherein the first server and the second server are mini-servers.

40. (New) The vendor computer according to claim 37, wherein the first server message and the second server message are mini-server messages.

41. (New) A method for performing secure electronic transactions on a computer network, said network comprising a buyers computer, a vendor server, a creditor server and a security server, said buyer's computer having a fingerprint file stored in the memory thereof, including:

i) said buyer computer requesting to purchase merchandise to said vendor server, said purchase request including said buyer computer's IP address;

ii) said buyer computer selecting a predetermined form of secured payment method;

iii) said payment method selection causing said vendor server to transmit to said security server a request for confirmation of said buyer computer's identity at said buyer computer's IP address;

iv) said confirmation request causing said security server to send a retrieval request to said IP address, said retrieval request including a retrieval program for detecting and retrieving said buyer's computer's fingerprint file, and said retrieval request further comprising a response request asking for confirmation of said purchase request; whereby a positive response from said buyer's computer to said security server accompanied by said fingerprint file causes said security server to confirm said buyer computer's identity to said vendor sewer and to approve said purchase.

42. (New) A method of performing secure electronic transactions on a computer network, said network comprising a buying computer, an ISP computer and a vendor computer, including:

said ISP computer assigning to buying computer a Buyer-ID code and 1P address;

said buying computer communicating via said ISP computer with said vendor computer and allowing an operator to select merchandise or services for purchase;

said Buyer-ID and buyer computer's IP address are provided to vendor computer programmed to request and receive said information;

vendor computer is programmed to use Buyer-ID and BC's current IP address along with information such as desired Item ID, cost and name for generating an electronic purchase inquiry which is transmitted to ISP computer;

ISP is programmed such that upon receipt of purchase Inquiry from MC, ISP uses combination of IP address and Buyer-ID to determine within ISP's Internal network whether Buyer IS in fact still online at the address assigned at the beginning of the online session;

whereby if buyer computer is determined to be connected to ISP computer at correct address, ISP computer then generates and transmits Transaction Confirmation Number and instructs MC to generate and forward invoice to ISP compute